Governo dos EUA luta contra empecilhos para destravar smartphones

Houve um dia em que os órgãos de segurança dos EUA ficaram felizes. Uma nova ferramenta, a GrayKey, uma caixinha composta de *hardware* e *software*, permitiu aos investigadores criminais furar o bloqueio de senhas e criptografias de iPhones.

A polícia de Indiana, por exemplo, destravou, de uma tacada, 96 iPhones apreendidos de suspeitos. Encontrou provas que incriminaram alguns suspeitos e provas que eximiram outros de responsabilidade.

Departamentos de polícia de outros estados, como Maryland, Oregon e Minnesota, ao saber da notícia, compraram a caixinha imediatamente, por US$ 15 mil a peça. O DEA se animou mais e anunciou que ia adquirir uma GrayKey mais sofisticada por US$ 30 mil. Mais departamentos de polícia e o FBI se interessaram.

Mas a alegria durou pouco. A Apple tratou de proteger seu produto, o iPhone, e a confiança dos consumidores, que, por qualquer razão, valorizam sua privacidade. Se usam senha e criptografia para proteger seus dados, não querem que ninguém venha a bisbilhotá-los — nem mesmo a polícia.

Assim, a Apple criou um recurso, em versão beta, para o sistema operacional iOS 11.4.1 do iPhone, que neutralizou a ação do GrayKey. O "modo restrito USB" requer que um telefone seja destravado dentro do período de uma hora, antes de qualquer transferência de dados pela porta de carregamento.

O GrayKey tem dois cabos acoplados na parte dianteira para a conexão de dois iPhones. Mas de um iPhone com "modo restrito USB" não sai nada. A não ser uma mensagem, que só serve para o dono do telefone, se ele mesmo quiser fazer transferências de dados.

"Destrave o iPhone para permitir que acessórios USB se conectem, quando passou mais de uma hora desde que o iPhone foi bloqueado", diz a mensagem. Aparece outra mensagem que qualquer intruso — incluindo as bem-intencionadas autoridades policiais — não devem gostar nada: "Apagar todos os dados deste iPhone após 10 digitações de código incorretas".

Nos EUA, a sensação que se tem é a de que os órgãos de segurança e as empresas de tecnologia estão metidos em um jogo de gato e rato. Os órgãos de segurança, com o apoio decidido do governo, querem ter acesso aos dados de *smartphones* a qualquer preço, para ajudar a solucionar crimes, suspeitas de terrorismo etc. — e tomam uma iniciativa após a outra.

O Vale do Silício — uma referência às empresas de tecnologia — contra-ataca com o desenvolvimento de novos recursos de segurança e com ações na Justiça. As empresas não querem abrir brechas a suspeitas de que seus dispositivos não são seguros — ou incapazes de garantir a privacidade do consumidor.

O Departamento de Justiça dos EUA pediu um gesto de boa vontade das empresas. Sugeriu que elas poderiam criar uma forma exclusiva de os órgãos de segurança quebrarem senhas e também comunicações e dados criptografados. Queria que as empresas criassem uma *backdoor* (porta dos

fundos), que poderia assegurar a integridade dos dados, mas que facilitasse o acesso dos órgãos de segurança com autoridade legal.

Entretanto, as empresas descartaram a ideia. Receberam o apoio de um ex-integrante do Conselho de Segurança Nacional da Casa Branca, Ari Schwartz, que agora é diretor administrativo da Venable, empresa que presta serviços de segurança cibernética.

“Requerer uma *backdoor* é uma má ideia para a segurança. Pode ajudar os órgãos de segurança em certos casos, em curto prazo, mas será muito ruim para a segurança em geral”, disse.

A preocupação é que, uma vez que uma *backdoor* é criada, será apenas uma questão de tempo para “atores nefários” conseguirem explorar a vulnerabilidade intencional. Schwartz disse ao *New York Times* que é preciso continuar criando sistemas seguros, mas, ao mesmo tempo, dar aos órgãos de segurança mais ferramentas para combater o crime.

Tais ferramentas poderiam incluir até mesmo o *hacking* com maior supervisão. Ou se arrumar uma maneira de os órgãos de segurança trabalharem juntos com as empresas de tecnologia.

Mas isso também não está na pauta das empresas, por enquanto. Por hora, os órgãos de segurança continuam batendo na porta da Justiça, pedindo a ela que bata na porta das empresas para pedir mais do que uma xícara de provas.

As empresas dizem que o governo não tem nada do que reclamar, porque elas estão cooperando — na medida do possível. A Apple diz que recebeu “requisições” da Justiça relacionadas a 4.450 dispositivos, entre mandados de busca e apreensão, ordens de escuta telefônica, registros de números discados e intimações. Afirma que atendeu 80% das requisições.

O Facebook declarou que atendeu 85% das requisições da Justiça. O Google declarou que 82% das requisições resultaram na produção de alguns dados para o governo. Ninguém está falando em 100%, lamentam os órgãos de segurança.

Nesse jogo de gato e rato, por falta de uma solução ganha-ganha, os órgãos de segurança se sentem em desvantagem. Afirmam que estão brigando no escuro, porque, mesmo que consigam apreender comunicações ou dados legalmente, é impossível lê-los por causa da criptografia.

Nos últimos anos, a Apple e o Google adicionaram criptografia como um recurso padrão em seus dispositivos. Ao mesmo tempo, outros produtos como Skype, WhatsApp e Signal adotaram comunicações criptografadas, que se tornaram comuns e fáceis de usar.

Date Created
17/10/2018